

CLAIMS:

1. A method of generating authentication data for authenticating a physical object; the method including:
 - measuring a property set Y of the object using a measurement procedure;
 - creating a property set I from the measured property set Y that meet a
 - 5 predetermined robustness criterion;
 - creating a property set A from the property set I that includes less information on the actual properties than property set Y ;
 - generating a control value V in dependence on properties of the property set A and inserting the control value in the authentication data.
 - 10
2. A method as claimed in claim 1, wherein the step of creating the property set A includes performing a contracting transformation.
3. A method as claimed in claim 2, wherein the contracting transformation
- 15 transforms a property to a binary number representative of a sign of the property.
4. A method as claimed in claim 1, wherein the step of creating the property set A includes selecting a subset of the property set I .
- 20 5. A method as claimed in claim 4, including creating helper data W for controlling the selection of the subset and inserting the helper data W in the authentication data.
6. A method as claimed in claim 5, including creating unique helper data W for
- 25 respective authentication applications.
7. A method as described in claim 1, wherein the predetermined robustness criterion is based on a signal to noise ratio of the measured properties and the step of creating the property set I includes performing a transformation Γ on the property set Y to create

disjunct property sets I_1 and I_2 where a signal to noise ratio of properties of I_1 are estimated to be higher than a signal to noise ratio of properties of I_2 ; and using I_1 as the property set I .

8. A method as claimed in claim 7, wherein the transformation Γ is a linear
5 transformation that converts a vector representing the property set Y to a vector with components α_i representing the set I , where each vector component α_i is independent of the other vector components α_j ($j \neq i$) and wherein the vector components are sorted according to an estimated signal to noise ratio.
- 10 9. A method as claimed in claim 7, including the step of creating the transformation Γ in dependence on a statistical property of the measurement procedure.
10. A method as claimed in claim 9, wherein the statistical property includes a covariance matrix derived from estimated properties X of the object and a corresponding
15 statistical distribution F .
11. A method as claimed in claim 7, including deriving a threshold from a noise level in the measured property set and assigning created properties with an absolute value larger than the threshold to set I_1 .
20
12. A method as claimed in claim 1, wherein the step of creating the control value V includes performing a cryptographic function on properties of the property set A .
13. A method as claimed in claim 12, wherein the cryptographic function is a one-
25 way function.
14. A computer program product operative to cause a processor to perform the method of claim 1.
- 30 15. A method of authenticating a physical object; the method including:
measuring a property set Y of the object using a measurement procedure;
creating a property set I from the measured property set Y that meet a predetermined robustness criterion;

creating a property set A from the property set I that includes less information on the actual properties than property set Y ;

generating a control value V' in dependence on properties of the property set A ,

5 retrieving a control value V that has been generated for the physical object during an enrolment; and

authenticating the physical object if there is a predetermined correspondence between the generating a control value V' and the retrieved control value V .

10 16. A computer program product operative to cause a processor to perform the method of claim 15.

17. A system (100) for authenticating a physical object (105); the system including an enrolment device (110), an authentication device (140), and a storage (130) for
15 storing authentication data;

the enrolment device (110) including:

an input (112) for receiving a property set Y of the object measured using a measurement procedure;

a processor (114) for creating a property set I from the measured
20 property set Y that meet a predetermined robustness criterion; creating a property set A from the property set I that includes less information on the actual properties than property set Y ; and generating a control value V in dependence on properties of the property set A ; and

an output (116) for supplying the control value to the storage as part of the authentication data; and

25 the authentication device (120) including:

an input (142) for receiving a property set Y of the object measured using a measurement procedure and for receiving a control value V from the storage;

a processor (144) for creating a property set I from the measured
property set Y that meet a predetermined robustness criterion; for creating a property set A
30 from the property set I that includes less information on the actual properties than property set Y ; for generating a control value V' in dependence on properties of the property set A ; and for authenticating the physical object if there is a predetermined correspondence between the generating a control value V' and the retrieved control value V ; and

an output (146) for issuing a signal indicating whether or not the physical object has been authenticated.

18. An authentication device (140) for use in a system as claimed in claim 17; the authentication device including:

an input (142) for receiving a property set Y of a physical object measured using a measurement procedure and for receiving a control value V from a storage;

a processor (144) for creating a property set I from the measured property set Y that meet a predetermined robustness criterion; for creating a property set A from the property set I that includes less information on the actual properties than property set Y ; for generating a control value V' in dependence on properties of the property set A ; and for authenticating the physical object if there is a predetermined correspondence between the generating a control value V' and the retrieved control value V ; and

an output (146) for issuing a signal indicating whether or not the physical object has been authenticated.